# China Cybersecurity Cooperation Affirmative

## Plan

### 1AC — Plan Text

#### The United States federal government should deepen bilateral cybersecurity negotiations with the People’s Republic of China to expand cooperation between U.S. and Chinese Computer Emergency Response Teams with the goal of achieving a joint protocol and concrete compliance framework.

## Solvency

### FYI Cards

#### FYI: CERT = CSIRT = nCSIRT

Morgus et. al 15 — Rober Morgus, a policy analyst with New America’s Cybersecurity Initiative, a member of the Global Commission on Internet Governance's Research Advisory Network, received his B.A. with honors in Diplomacy and World Affairs from Occidental College, and Isabel Skierka, a research associate with the Global Public Policy Institute (GPPi), was a Carlo Schmid fellow at the North Atlantic Treaty Organization, where she worked on the Alliance’s Smart Defence Initiative, has a master’s in international conflict studies at the war studies department of King’s College London and holds a bachelor’s degree in European studies from Maastricht University, and Mirko Hohmann, a research associate with the Global Public Policy Institute, holds a Master of Public Policy from the Hertie School of Governance in Berlin and a Bachelor of Arts in international affairs from the University of St. Gallen, Switzerland, and Tim Maurer, Former Director of the Global Cybersecurity Norms and Resilience Project and Head of Research, Cybersecurity Initiative, holds a Master in Public Policy concentrating on international and global affairs from the Harvard Kennedy School, 2015 (“National CSIRTs and their Role in Computer Security Incident Response,” *New America Foundation*, November, Available Online at <https://www.newamerica.org/documents/1431/CSIRTs-incident-response.pdf>, Accessed 06-27-2016, p. 10, AS)

In addition to residing in governmental ministries, some nCSIRTs are part of a national cybersecurity center, like US-CERT, which resides in the National Cybersecurity and Communication Integration Center (NCCIC) or CERT Australia, which is co-located with other Australian government organizations' cyber security capabilities in the Australian National Cyber Security Center. Other governmental nCSIRTs are part of a government institution but have public–private governance structures and participation, like NCSC.nl in the Netherlands and CERT.at in Austria.

#### FYI: US-CERT functions as a national CERT, not just a governmental CERT — it protects the civilian and private sector

US-CERT No Date — United States Computer Emergency Readiness Team, a part of the U.S. Department of Homeland Security, no date ("About Us," *US-CERT.gov*, Available Online at https://www.us-cert.gov/about-us, Accessed 06-27-2016, AS)

In early 2000, Federal Government networks began to experience an alarming number of cyber breaches. In response, Congress created the Federal Computer Incident Response Center (FedCIRC) at the General Services Administration as a centralized hub of coordination and information sharing between federal organizations. With the creation of the Department of Homeland Security in 2002, Congress transferred these responsibilities to the new Department. In 2003, FedCIRC was renamed “US-CERT,” and its mission was expanded to include providing boundary protection for the federal civilian executive domain and cybersecurity leadership. This shared responsibility has evolved over time to make US-CERT a trusted partner and authoritative source in cyberspace for the Federal Government; SLTT governments; private industry; and international organizations.

For further clarification of the difference between a national CERT and a governmental one, look to the Hathaway evidence.

### 1AC — Solvency

#### CERT cooperation exists but is largely undefined — no categorization of CSIRT functions.

Morgus et. al 15 — Rober Morgus, a policy analyst with New America’s Cybersecurity Initiative, a member of the Global Commission on Internet Governance's Research Advisory Network, received his B.A. with honors in Diplomacy and World Affairs from Occidental College, and Isabel Skierka, a research associate with the Global Public Policy Institute (GPPi), was a Carlo Schmid fellow at the North Atlantic Treaty Organization, where she worked on the Alliance’s Smart Defence Initiative, has a master’s in international conflict studies at the war studies department of King’s College London and holds a bachelor’s degree in European studies from Maastricht University, and Mirko Hohmann, a research associate with the Global Public Policy Institute, holds a Master of Public Policy from the Hertie School of Governance in Berlin and a Bachelor of Arts in international affairs from the University of St. Gallen, Switzerland, and Tim Maurer, Former Director of the Global Cybersecurity Norms and Resilience Project and Head of Research, Cybersecurity Initiative, holds a Master in Public Policy concentrating on international and global affairs from the Harvard Kennedy School, 2015 (“National CSIRTs and their Role in Computer Security Incident Response,” *New America Foundation*, November, Available Online at <https://www.newamerica.org/documents/1431/CSIRTs-incident-response.pdf>, Accessed 06-27-2016, p. 11-12, AS)

Though some coordination in the operations of nCSIRTs has occurred, there remains a great deal of uncertainty regarding the standardization of the role of nCSIRTs. When building CERT-UK, the United Kingdom’s nCSIRT, the UK Cabinet Office identified 47 possible functions of an nCSIRT, but it ultimately prioritized only four of these functions in the creation of CERT-UK.32 Nonetheless, the defining feature of an nCSIRT [end page 11] – similar to operationally focused CSIRTs in the private sector and elsewhere that primarily remediate damage and recover and rebuild systems – is its incident response function. Exceptions to this are nCSIRTs that double as governmental CSIRTs and are responsible for remediation, recovery and rebuilding of government networks. But most nCSIRTs focus much more on the coordination of response and information sharing and dissemination, unlike smaller CSIRTs in the private sector or government. In this coordinating function, an nCSIRT does not have a direct, operational role, but more of an advisory role. It receives, analyzes and synthesizes incident and vulnerability information disseminated by other CSIRTs. It then re-distributes this processed information to its constituency through bulletins or a shared database.

In the US, US-CERT is operationally responsible for federal government networks and has a coordinating role as the national point of contact for domestic and international stakeholders. It operates alongside the Industrial Control Systems CERT, which coordinates incident response among critical infrastructure owners and operators. Germany’s national information security agency (BSI) operates the national governmental CSIRT that serves as an authorized national point of contact, and also runs Bürger-CERT, which provides citizens and small enterprises with email updates on IT-related threats and vulnerabilities. Luxembourg, on the other hand, splits governmental and national tasks and operates GOVCERT.LU, which is responsible for governmental networks only, and CIRCL, which is responsible for private sector and non-governmental entities in Luxembourg and serves as the nCSIRT. Additionally, some nCSIRTs serve as the “response team of last resort,” either redirecting a case to the CSIRT responsible for handling it or providing some degree of support itself. The service portfolio of CSIRTs has been described in detail in a number of publications,33 but the categorization of CSIRT functions was being reconsidered in a FIRST committee at the time of writing this report,34 and a clear delineation of functions specific to nCSIRTs does not exist.

#### China says yes — they’ve cooperated before on the same subject.

Gady 15 — Franz-Stefan Gady, Senior Fellow and Foreign Policy Analyst at the East-West Institute, Editor at *The Diplomat,* M.A. in International Relations from John Hopkins University, B.A. in International Relations from Weber University, 2015 (“Can the US and China Cooperate on the First (and Last) Line of Cyber Defense?,” *The Diplomat,* October 30th, Accessible Online at <http://thediplomat.com/2015/10/can-the-us-and-china-cooperate-on-the-first-and-last-line-of-cyber-defense/>, Accessed On 06-22-2016, MA)

That China is willing to cooperate more closely with other countries can be seen with Beijing’s participation in yearly joint cyber exercises – the Cyber Exercise Drill – organized by the Asia Pacific Computer Emergency Response Team (APCERT). The aim of these “blind drills” is to coordinate international responses to cyberattacks. The exercises specifically deal with improving communication protocols, information sharing, and crisis response times of the CERTs participating.

As an initial first step, the United States could join the drill and apply the lessons learned on the multilateral level to the Sino-U.S. bilateral level. (In the past, APCERT has extended invitations to the Organization of the Islamic Cooperation-Computer Emergency Response Team and the European Government Computer Security Incident Response Teams).

Cooperation between countries is possible, and this has been exemplified in the field of cybercrime. There, Beijing and Washington have cooperated on multiple occasions in the past. The last time, a few weeks prior to the Obama-Xi meeting in Washington D.C. in September, the Chinese government agreed to arrest a number of Chinese hackers at the request of the U.S. government.

## Cybersecurity Advantage

### 1AC — Cybersecurity Advantage

#### Contention \_: Cybersecurity

#### First, despite the recent U.S.-China cyberespionage agreement hacks are still happening

Daugirdas and Mortenson 15 — Kristina Daugirdas, Assistant Professor of Law at the University of Michigan, was awarded the Francis Deák Prize for an outstanding article published in the American Journal of International Law, serves as co-editor of the Contemporary Practice of the United States section of the American Journal of International Law, and Julian Davis Mortenson, Professor of Law at the University of Michigan, co-editor of the "Contemporary Practice of the United States" section of the American Journal of International Law, one of the principal drafters of the merits briefs in the landmark case Boumediene v. Bush, 2015 (“Contemporary Practice of the United States Relating to International Law: General International and U.S. Foreign Relations Law: United States and China Reach Agreement Regarding Economic Espionage and International Cybersecurity Norms,” *American Journal of International Law* (109 A.J.I.L. 878), October, Available Online to Subscribing Institutions via Lexis-Nexis, Accessed 06-22-2016, AS)

Obama and Xi reached the agreement during their talks at the White House on September 24-25. n7 But the substance of the agreement had been "in the works" several weeks before that, with discussions beginning after China's alleged theft of records from the Office of Personnel Management, and continuing when National Security Advisor Susan E. Rice traveled to Beijing in late August to prepare for Xi's visit to the White House. n8 Following those conversations, Secretary of the Central Political and Legal Affairs Commission of the Communist Party of China Meng Jianzhu--acting as a Special Envoy for Xi--met with senior administration officials in Washington from September 9-12 to discuss cybersecurity issues, n9 leading to "substantial agreement" on those topics, including Chinese economic espionage. n10 At the time, [\*881] administration officials characterized those talks as "pretty blunt" and "pretty ugly," n11 and it was unclear whether a final agreement would be reached during Xi's visit. n12

According to press reports, China agreed to affirm the norm against economic cyberespionage in part because it was "rattled" by the threat of U.S. sanctions. n13 Last April, Obama had issued an executive order permitting the imposition of sanctions on individuals or entities that engage in malicious cyberenabled activities, including economic espionage, that threaten the United States' interests. n14 So far no such sanctions have been imposed, but press reports indicated that the administration was contemplating sanctions on Chinese companies and individuals. n15 An administration official acknowledged that the United States decided to refrain from issuing any sanctions prior to Xi's visit, in light of the progress made during the discussions between Meng and senior administration officials. n16 Such sanctions do remain a possibility, however. During Xi's visit, Obama reiterated that the administration "will apply [sanctions] and whatever other tools [the United States] ha[s] in [its] toolkit to go after cyber criminals, either retrospectively or prospectively," where there is "proof that they've gone after U.S. companies or U.S. persons." n17

In his announcement of the agreement, Obama noted that the primary question is now whether China's "words [will be] followed by actions." n18 Indeed, at a congressional hearing several days after the agreement was reached, Deputy Secretary of Defense Robert Work said, "I think all of us have some healthy skepticism about this, but I believe it's a good confidence-building measure and a good first step, and we will see if it leads to better behavior on the part of the Chinese." n19 Explaining the agreement, Work said:

[\*882] [O]ne hopes that . . . this agreement may create the space for us to have a--more than a conversation, but one that would lead to some kind of a change in behavior on the part of these state actors. . . . [W]hat we have done [after identifying the source of a cyber attack] is, we have confronted China, and China, in some cases, has said, "Look, this was a hacker that was insider our country, but we had no control over him." What this [agreement] allows us to do is say, "Okay, well, what are you going to do about that? That's a cybercrime. Are you going to provide us the information we need to prosecute this person? Are you going to take care of it on your own?" n20

In the weeks after the agreement was reached, China arrested several Chinese hackers that U.S. officials had identified as having stolen commercial secrets from U.S. firms with the intention of giving or selling that information to Chinese state-run companies. n21 A report by private researchers showed, however, that hackers linked to the Chinese government have continued to try to acquire confidential information by accessing U.S. technology and pharmaceutical companies' networks. n22 Administration officials are aware of that report, but have declined to comment on it. n23 U.S. Cyber Command's Deputy Commander Lt. Gen. James K. McLaughlin pointed out that the elimination of Chinese economic cyberespionage will take time, and it may simply be "too early . . . to see any of th[e] changes" called for by the agreement. n24

#### Second, a CERT compliance framework paves the way for strong cooperation on cybersecurity and decreases the risk of cyber-catastrophe.

Gady 15 — Franz-Stefan Gady, Senior Fellow and Foreign Policy Analyst at the East-West Institute, Editor at *The Diplomat,* M.A. in International Relations from John Hopkins University, B.A. in International Relations from Weber University, 2015 (“Can the US and China Cooperate on the First (and Last) Line of Cyber Defense?,” *The Diplomat,* October 30th, Accessible Online at <http://thediplomat.com/2015/10/can-the-us-and-china-cooperate-on-the-first-and-last-line-of-cyber-defense/>, Accessed On 06-22-2016, MA)

To avoid past mistakes, the rather vague September agreement needs to be followed up as soon as possible by bilateral meetings to more clearly define specific venues of cooperation between China and the United States.

And while the September agreement talks about a meeting of a new joint China-U.S. high-level government-to-government working group to combat cybercrime to be held before the end of the 2015 and biannually in subsequent years, other initiatives to deepen cooperation between the two countries need to happen.

One possible way to do so is to strengthen cooperation between the Chinese and U.S. Computer Emergency Response Teams (CERTs). In general, CERTs are the first (and last line) of defense in protecting a country’s critical information infrastructure from cyberattacks and are tasked with coordinating responses to network intrusions across the nation and beyond.

China’s CERT is specifically tasked with “building up the national monitoring, warning, emergency response, evaluation and public opinion centers for network security.” It serves as the coordinating body for other CERTs in China and also engages with CERTs in other countries.

Of particular note here is the cooperation between the CERTs of China, Japan, and South Korea. The CERTs meet annually, share information including threat data, have established a 24/7 technical hotline, and purportedly have a protocol for crisis escalation in place in the event of major cyberattacks. Representatives of the three countries recently met in Seoul to better coordinate their cyber policies when it comes to fighting cybercrime and terrorism.

China and the United States have also been cooperating on a CERT level over the last couple of years, but at a rather ad-hoc and impromptu level, which has substantially undermined collaboration. For example, up until now no joint protocol exists for how to handle requests for information or what type of information needs to be provided for one side to take action when an incident occurs.

#### Third, US-China cooperation solves cyber norms.

Lieberthal and Singer 14 — Kenneth Lieberthal, a senior fellow in Foreign Policy and Global Economy and Development at Brookings, former professor at the University of Michigan, has a bachelor’s from Dartmouth College, and a master’s and doctorate in political science from Columbia University, and Peter W. Singer, Senior Fellow at the Brookings Institution, Director of the Center for 21st Century Security and Intelligence at the Brookings Institution, received his Ph.D. in Government from Harvard University and an A.B. from Princeton's Woodrow Wilson School of Public and International Affairs, 2014 (“Cybersecurity and U.S.-China Relations,” *John L. Thornton China Center* and *21st Century Defense Initiative* at *Brookings*, February, 06-29-2016, MA)

But the United States and China are the two most significant national players in this sphere. Moreover, these two leading states represent very different views on the proper use and future of the Internet. We therefore feel that thinking through these issues in a U.S.-China context can provide a useful way to develop approaches that should then be discussed more broadly, with the goal of ultimately establishing global norms and implementing mechanisms to bring greater order and security to those parts of the cyber realm where this is feasible.

More importantly, the spillover effect of cybersecurity on the broader U.S.-China relationship is also perhaps more critical than for any other bilateral relationship. This is both because of the enormous importance of U.S.-China relations in the emerging world order and, in turn, the growing role of cyber issues in eroding strategic trust and poisoning public and elite attitudes. If this trend can be reversed through improved engagement by the U.S. and China on cybersecurity, the outcome would be a “triple win.” It would bolster U.S.-China bilateral relations, serve as a crucial building block for multilateral efforts in the cyber arena, and also aid in broader US-Chinese engagement on other issues of importance, like global finance and the environment, where the two nations must learn to work better together.

#### Fourth, unclear norms ensure escalation — arms races and false flag attacks.

Rosenzweig 9 — Paul Rosenzweig, Professor of Law at Georgetown University, Senior Advisor to the Chertoff Group on National Security, Deputy Assistant Secretary for policy at the US Department of Homeland Security, 2009 (“National Security Threats in Cyberspace," *American Bar Association Standing Committee on Law and National Security*, September, Accessible Online at [www.utexas.edu/law/journals/tlr/sources/Issue%2088.7/Jensen/fn137.Rosenwieg.pdf](http://www.utexas.edu/law/journals/tlr/sources/Issue%2088.7/Jensen/fn137.Rosenwieg.pdf), Accessed On 01-26-2016, MA)

Offensive dominance creates a great risk of cyber arms races. State and non-state actors are likely to view the prevalence of offensive cyber threats as a legitimate rationale for bolstering their own capabilities, both defensive and offensive, thus fueling an action-reaction dynamic of iterative arming. Experts believe that at least 20 nations are engaged in a cyber arms competition and possess the type of advanced capabilities needed to wage cyber war against the United States.121 As Michael Nacht, Former Assistant Secretary of Defense for Global Strategic Affairs, told us, “An arms race is already going on in cyberspace and it is very intense.”122 Conflict in cyberspace is uniquely predisposed to escalation given uncertainties about what constitutes an act of war and the growing number of state and non-state actors seeking offensive capabilities. Actors are more likely to misperceive or miscalculate actions in cyberspace, where there is no widely understood strategic language for signaling intent, capability and resolve.123 Uncertainty will encourage states to prepare for worst-case contingencies, a condition that could fuel escalation. Furthermore, “false flag” attacks, in which an actor purposefully makes an attack look like it came from a third party, could also ignite a conflict.124

#### Finally, cyberattacks escalate and provoke retaliation — misattribution undermines checks on conflict.

Dycus 10 — Stephen Dycus, Professor of Law at the University of Vermont, Visiting Professor of National Security at the United States Military Academy, M.A. in Legal Studies from Harvard University, 2010 (“Congress’s Role in Cyber Warfare,” *Journal of National Security Law & Policy*, Vol. 4, No. 155, August 11th, Accessible Online at <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>, Accessed On 06-29-2016, MA)

The term “cybersecurity” might be understood to refer to defense against cyber attacks. “Cyber attack” suggests offensive use, but the label is inexact and might be misleading. A preemptive strike to ward off an imminent enemy attack is considered defensive. Digital espionage might be part of the preparation for an attack, or it might be perceived that way by the target, which might then be provoked to defend itself by responding with a preemptive attack, either cyber or kinetic.

The important point here is that any use of cyber weapons, offensive or defensive, could have enormous consequences for the security and other interests of the United States. The effect of such use, actual or potential, matters more than the labels. And if the effect – on human life or property, for example, or diplomatic relations or compliance with the law of armed conflict – is substantial, Congress has a role to play in adopting policy for that use.

Congress has not thus far adopted measures suited to the regulation of cyber warfare. The War Powers Resolution, for example, is concerned with sending U.S. troops into harm’s way, rather than with clicking a computer mouse to launch a cyber attack, although the strategic consequences might be similar. And the WPR’s relatively relaxed timetable for executive notice and legislative response is unrealistic for war on a digital battlefield. Similarly, if cyber warfare is regarded as an intelligence activity, the intelligence oversight measures just described cannot, for reasons already indicated, ensure that Congress will be able to play a meaningful role. In the words of the National Research Council study cited above, “Today’s policy and legal framework for guiding and regulating the use of cyberattack is ill-formed, undeveloped, and highly uncertain.”

Our experience with nuclear weapons may point to needed reforms. Since the beginning of the Cold War, the United States has had a fairly clear nuclear policy (albeit one that deliberately includes an element of ambiguity) – one known generally to Congress, the American public, and potential enemies.46 Congress has approved or disapproved the purchase of the weapons and delivery systems. It has been briefed on the policy, and it has debated that policy vigorously.47 While Congress has not articulated U.S. nuclear policy in any coherent form, it has collaborated closely with the executive branch in the development and execution of that policy.

Cyber weapons bear a striking resemblance to nuclear weapons in some important ways. An enemy’s cyber attack would, like a nuclear strike, probably come without a clear warning. There are as yet no reliable defenses against either a cyber attack or a nuclear attack. Collateral damage from a nuclear attack would almost certainly be very extensive and would linger for an extended period.48 The direct and indirect effects of a cyber attack, while different in kind and degree, still could be widespread and indiscriminate.49

In other ways, cyber weapons are critically different from their nuclear counterparts. For one thing, the time frame for response to a cyber attack might be much narrower. A nuclear weapon delivered by a land-based ICBM could take 30 minutes to reach its target. An electronic attack would arrive instantaneously, and leave no time to consult with or even inform anyone outside the executive branch before launching a counterstrike, if that were U.S. policy. What most distinguishes digital warfare, however, is the potential difficulty in identifying the source of a cyber attack. It is always possible, of course, that an enemy might covertly deliver a nuclear device to the U.S. homeland in a shipping container or a Cessna. But the apparent ease with which a cyber attack may be carried out without attribution could make it impossible to fight back at all. If an attacker made it appear that the source was an innocent neutral state or perhaps another enemy of the attacker, a misdirected U.S. response might provoke a wider conflict. The potential difficulty in tracking the source also makes a policy of deterrence based on a threat of retaliation far less credible.

Given these characteristics of cyber warfare, and the continuing refinement of cyber weaponry, we approach a state of extreme strategic instability, with each nation on hair-trigger alert. The execution of an illconceived cyber war policy calling for a prompt response – or any response – to an attack or threatened attack could have disastrous, unanticipated consequences. It also might, depending on the circumstances, violate the law of armed conflict.

### 2AC — Grid Meltdown Impact

#### Cyber threat and grid meltdown is feasible — empirically proven

Pry 15 — Peter Pry, Executive Director of the Task Force on National and Homeland Security and Director of the U.S. Nuclear Strategy Forum, both Congressional Advisory Boards, and served on the Congressional EMP Commission, the Congressional Strategic Posture Commission, the House Armed Services Committee, and the CIA, author of the books "Blackout Wars", "Apocalypse Unknown", and "Electric Armageddon,” 2015 (“Cyber Hype?” *The Mackenzie Institute*, October 28th, Available Online at <http://mackenzieinstitute.com/cyber-hype/>, Accessed June 29, 2016//AW)

Tomorrow’s cyber super-threat, that with computer viruses and hacking alone can blackout the national electric grid for a year or more, and so destroy an entire nation, may already be upon us today. Admiral Michael Rogers on November 20, 2014, warned the House Permanent Select Committee on Intelligence that sophisticated great powers like China and Russia have the capability to blackout the entire U.S. national electric grid for months or years by means of cyber attack, according to press reports. Admiral Rogers, as Chief of U.S. Cyber Command and Director of the National Security Agency, is officially the foremost U.S. authority on the cyber threat. “It is only a matter of the when, not the if, that we are going to see something traumatic,” Admiral Rogers testified to Congress, as reported on CNN (November 21, 2014). However, Jonathan Pollett, a cyber-security expert, in an article challenged Admiral Rogers’ warning as wrong, or misunderstood and exaggerated by the press: “No, hackers can’t take down the entire, or even a widespread portion of the US electric grid. From a logistical standpoint, this would be far too difficult to realistically pull off,” writes Pollett in “What Hackers Can Do To Our Power Grid,” Business Insider (November 23, 2014). Yet, on March 31, 2015, Turkey’s national electric grid was temporarily blacked-out, briefly causing widespread chaos to businesses and society in a member of NATO and crucial U.S. ally in the Middle East. Reportedly, Iran caused the blackout by a cyber attack. But Turkey has not officially confirmed that Iran was the culprit. If so, it will be the first time in history that a nationwide blackout is confirmed as resulting from cyber warfare.

#### Grid meltdown creates chaos and has huge death tolls

Noory 15 — George Noory, host of Coast to Coast AM, previously the director of news planning and development at KSTP-TV in Minneapolis, 2015 (“EMP Grid Meltdown Could Destroy America,” *Coast to Coast AM*, September 23rd, Available Online at <http://www.coasttocoastam.com/article/emp-grid-meltdown-could-destroy-america>, Accessed June 29, 2016//AW)

As C2C previously reported, a recent Congressional study prepared by former Rep. Bartlett stated that 90 percent of all Americans might be dead within a year following an EMP generated grid meltdown. The federal government has finally introduced a bill, the Critical Infrastructure Protection Act, to toughen up the grid. But that may meet opposition, Fortschen warned, citing the last time a grid protection law was attempted it was killed by a lone Senator. And, not only are we vulnerable from the unpredictable forces of the sun, but America's enemies are said to be plotting a major EMP attack that could be "100 times worse than 9/11," Fortschen told George. Enemies with long range ICBM missiles could detonate a nuclear device in the upper atmosphere at key strategic locations, knocking out the grid with an EMP, Fortschen said. And a military response would be very slow to respond with "computerized planes falling from the skies," he said.

### Extend: Attack on Grid Likely

#### An EMP attack on the grid is likely and causes massive death tolls

Cooper and Pry 15 — Henry Cooper, former director of the Strategic Defense Initiative, Peter Pry, executive director of the EMP Task Force on National and Homeland Security and served in the EMP Commission, the House Armed Services Committee, and the Central Intelligence Agency, 2015 (“The Threat to Melt the Electric Grid,” *The Wall Street Journal*, April 30th, Available Online at <http://www.wsj.com/articles/the-threat-to-melt-the-electric-grid-1430436815>, Accessed on June 29, 2016//AW)

The Pentagon is moving the headquarters for the North American Aerospace Defense Command (Norad) back into Cheyenne Mountain near Colorado Springs, Colo., a decade after having largely vacated the site. Why the return? Because the enormous bunker in the hollowed-out mountain, built to survive a Cold War-era nuclear conflict, can also resist an electromagnetic-pulse attack, or EMP. America’s military planners recognize the growing threat from an EMP attack by bad actors around the world, in particular North Korea and Iran. An EMP strike, most likely from the detonation of a nuclear weapon in space, would destroy unprotected military and civilian electronics nationwide, blacking out the electric grid and other critical infrastructure for months or years. The staggering human cost of such a catastrophic attack is not difficult to imagine.

#### Chinese cyber-attack on the grid is likely

Crawford 14 — Jaime Crawford, CNN national security reporter who covers the Pentagon, 2014 (“The U.S. government thinks China could take down the power grid,” *CNN News*, November 21st, Available Online at <http://www.cnn.com/2014/11/20/politics/nsa-china-power-grid/>, Accessed on June 29, 2016//AW)

China and "probably one or two other" countries have the capacity to shut down the nation's power grid and other critical infrastructure through a cyber attack, the head of the National Security Agency told a Congressional panel Thursday. Admiral Michael Rogers, who also serves the dual role as head of U.S. Cyber Command, said the United States has detected malware from China and elsewhere on U.S. computers systems that affect the daily lives of every American. "It enables you to shut down very segmented, very tailored parts of our infrastructure that forestall the ability to provide that service to us as citizens," Rogers said in testimony before the House Intelligence Committee. Rogers said such attacks are part of the "coming trends" he sees based on "reconnaissance" currently taking place that nation-states, or other actors may use to exploit vulnerabilities in U.S. cyber systems. A recent report by Mandiant, a cyber-security firm, found that hackers working on behalf of the Chinese government were able to penetrate American public utility systems that service everything from power generation, to the movement of water and fuel across the country. "We see them attempting to steal information on how our systems are configured, the very schematics of most of our control systems, down to engineering level of detail so they can look at where are the vulnerabilities, how are they constructed, how could I get in and defeat them," Rogers said. "We're seeing multiple nation-states invest in those kinds of capabilities."

### They Say: “CERTs Don’t Solve Cyber Cooperation”

#### CERTs foster cooperation and de-escalate tensions — cyber “hotline”

Hathaway et. al. 15 — Melissa Hathaway, Senior Advisor for the Cyber Security Project for the Belfer Center for Science and International Affairs at the John F. Kennedy School of Government of Harvard University, has a B.A. degree from The American University in Washington, D.C., has completed graduate studies in international economics and technology transfer policy and is a graduate of the U.S. Armed Forces Staff College, with a special certificate in Information Operations, and Chris Demchak, co-director of the NWC Center for Cyber Conflict Studies (C3S), holds a PhD in Political Science from UC Berkeley and a MPA in Economic Development from Princeton, and Jason Kerben, a subject-matter expert on the Potomac Institute for Policy Studies’ Cyber Readiness Index project, also serves as senior advisor to multiple Departments and Agencies in matters related to information security and cyber security, and Jennifer McArdle, a Fellow in the Center for Revolutionary Scientific Thought at the Potomac Institute for Policy Studies, a PhD candidate at King’s College London in the War Studies department, and Francesca Spidalieri, Senior Fellow for Cyber Leadership at Salve Regina University, earned her B.A. in political science and international relations from the University of Milan and a M.A. in international affairs and security studies from Tufts University, 2015 (“Cyber Readiness Index 2.0: A Plan For Cyber Readiness: A Baseline and An Index,” *Potomac Institute for Policy Studies*, November, Available Online at <http://belfercenter.hks.harvard.edu/files/cyber-readiness-index-2.0-web-2016.pdf>, Accessed 06-27-2016, p. 12, AS)

National CSIRTs can also be used as a mechanism to build confidence between countries and foster cooperation. For example, China, Japan, and Korea—three countries that have historically experienced tensions—have developed a trilateral annual CSIRT meeting to discuss cyber incident response mechanisms. The meetings have helped instill confidence and trust resulting in the development of a cyber “hotline” to communicate on significant cyber incidents.40

Cyber incident response capabilities, joint meetings, and exercises are just a few of the basic mechanisms that can help a country proactively prepare for and mitigate the ripple effects of a major cyber incident. CSIRTs increase a country’s speed, recovery, and resilience against cyber threats, reducing the likely overall economic and operational impact of nationally significant attacks or campaigns. Some of the key preconditions for the successful deployment of these incident response teams are a well trained staff, and effective rapidly deployable tools. This facilitates an incident response team’s ability to foster cooperation and coordination in incident prevention, enable rapid reaction to incidents, and promote information sharing among stakeholders, both domestically and internationally.

### They Say: “Doesn’t Solve Cyberattacks”

#### CERT cooperation resolves cyberattacks while creating stable inter-state communication channels

Maurer 15 — Tim Maurer, Former Director of the Global Cybersecurity Norms and Resilience Project and Head of Research, Cybersecurity Initiative, holds a Master in Public Policy concentrating on international and global affairs from the Harvard Kennedy School, 2015 ("The Challenges Facing Computer Security Incident Response Teams," *Council on Foreign Relations*, July 20th, Available Online at http://blogs.cfr.org/cyber/2015/07/20/the-challenges-facing-computer-security-incident-response-teams/, Accessed 06-27-2016, AS)

CSIRTs have been a cornerstone of cyber incident response for decades. Also known as Computer Emergency Response Teams (CERTs), CSIRTs are teams of technical experts with the mission to maintain and protect the security of their customers’ computer networks and systems that rely on it. For example, when the OpenSSL Heartbleeed vulnerability was discovered last year, which security expert Bruce Schneier called a “catastrophic bug,” US-CERT issued an alert and a white paper containing an overview of the systems affected, a description of the threat, and recommendations for solutions and mitigation. US-CERT worked with private sector partners, the FBI, Financial Services Information Sharing and Analysis Center, and Canadian Cyber Incident Response Center to prepare and disseminate alerts. CSIRTs, can be based at private companies, governments, universities or other organizations.

While their primary mission is technical in nature, they are under growing pressure to accommodate various policy and political objectives of the countries in which they are located.

A growing number of governments have been setting up national CSIRTs to coordinate CSIRT activity within their borders. Additionally, CSIRTs are increasingly referenced in cyber norm discussions at the United Nations and the Organization for American States. Cybersecurity capacity building efforts now routinely include programming aimed at creating national CSIRTs and strengthening cooperation between existing ones.

All of these activities raise a number of important policy questions: What constitutes a national CSIRT? How is it institutionalized? How should it function in countries with existing CSIRTs? Should it coordinate a national response to a major cyber incident and if so, how?

These are some of the questions we put to the CSIRT representatives at the FIRST conference[\*] as part of our CSIRT project. During the discussion, we explored ways to improve the policy and technical communities’ understanding on the role of CSIRTs. It became clear that cooperation between national CSIRTs can serve as a communication channel for countries with otherwise strained diplomatic relations and can help build confidence between them to improve network security. An example for collaboration is APCERT, a coalition of CSIRTs from thirteen economies across the Asia Pacific region, including the Japanese, Korean and Chinese national CSIRTs.

\*Note to debaters: the FIRST conference — The Forum of Incident Response and Security Teams (FIRST) conference

#### US CSIRT is key to cyber readiness and national security

Hathaway et. al. 15 — Melissa Hathaway, Senior Advisor for the Cyber Security Project for the Belfer Center for Science and International Affairs at the John F. Kennedy School of Government of Harvard University, has a B.A. degree from The American University in Washington, D.C., has completed graduate studies in international economics and technology transfer policy and is a graduate of the U.S. Armed Forces Staff College, with a special certificate in Information Operations, and Chris Demchak, co-director of the NWC Center for Cyber Conflict Studies (C3S), holds a PhD in Political Science from UC Berkeley and a MPA in Economic Development from Princeton, and Jason Kerben, a subject-matter expert on the Potomac Institute for Policy Studies’ Cyber Readiness Index project, also serves as senior advisor to multiple Departments and Agencies in matters related to information security and cyber security, and Jennifer McArdle, a Fellow in the Center for Revolutionary Scientific Thought at the Potomac Institute for Policy Studies, a PhD candidate at King’s College London in the War Studies department, and Francesca Spidalieri, Senior Fellow for Cyber Leadership at Salve Regina University, earned her B.A. in political science and international relations from the University of Milan and a M.A. in international affairs and security studies from Tufts University, 2015 (“Cyber Readiness Index 2.0: A Plan For Cyber Readiness: A Baseline and An Index,” *Potomac Institute for Policy Studies*, November, Available Online at <http://belfercenter.hks.harvard.edu/files/cyber-readiness-index-2.0-web-2016.pdf>, Accessed 06-27-2016, p. 9, AS)

2. INCIDENT RESPONSE

The second essential element that indicates a country’s cyber readiness involves establishing and maintaining an effective national incident response capability. Often, this capability takes the form of one or more National Computer Security Incident Response Teams (National CSIRTs) or Computer Emergency Response Teams (CERTs)—hereinafter referred to collectively as CSIRTs—responsible for managing incident response in the event of natural or manmade cyber-related disasters that affect critical services and information infrastructures.22 At present, one hundred and two national CSIRTs have been established worldwide and another four CSIRTs are under development.23 CSIRT teams usually consist of a blend of IT security experts and practitioners from academia, the private sector, and government. In addition to providing the specifc technical competence to respond to cyber incidents of national interest, these incident response teams strengthen the ability of a national government to understand and combat cyber threats. Operating a National CSIRT, therefore, forms a core component of a country’s overall strategy to secure and maintain the services and infrastructures that are vital to national security and economic growth.24

National CSIRTs, unlike strictly governmental ones, serve a broad constituency ranging from government departments to private and public entities to citizens. A well-established National CSIRT provides reactive services above all else—i.e., the ability to respond to incidents by containing and mitigating incidents as they occur.25 Although the specifc organizational form of National CSIRTs may vary, and not every country may have the same needs and resources, these specialized and dedicated units should provide a series of both proactive and reactive functions, as well as preventive, educational, and security quality management services. These services include, but are not limited to: establishing shared understanding of the threats facing the country; publishing alerts and advisories on cyber vulnerabilities and threats; promoting cyber security awareness and best practices; identifying, detecting, containing, and managing security threats and preparing for potential incidents; coordinating incident response activities; analyzing computer security incidents and providing feedback and lessons learned (for shared learning); promoting activities that increase resilience; and supporting the national cyber security strategy.

### They Say: “Cyberattacks Declining”

#### September agreement didn’t stop cyber espionage — more to come

Gady 16 — Franz-Stefan Gady, Senior Fellow and Foreign Policy Analyst at the East-West Institute, Editor at The Diplomat The Diplomat, 2016 ("Top US Spy Chief: China Still Successful in Cyber Espionage Against US," *The Diplomat*, February 16th, Available Online at http://thediplomat.com/2016/02/top-us-spy-chief-china-still-successful-in-cyber-espionage-against-us/, Accessed 06-30-2016, MW)

Last week, the Director of National Intelligence, James R. Clapper, delivered his annual threat briefing to the Senate Armed Forces Committee noting that China remains engaged in malicious activities in cyberspace against the United States, despite a U.S.-Chinese bilateral agreement to refrain from conducting or knowingly supporting commercial cyber-espionage. “China continues to have success in cyber espionage against the U.S. government, our allies, and U.S. companies,” Clapper emphasized. “Beijing also selectively uses cyberattacks against targets it believes threaten Chinese domestic stability or regime legitimacy.” Clapper goes on to say that U.S. intelligence agencies will monitor China’s compliance with the September 2015 bilateral agreement to refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property with the intent of providing competitive advantage to companies or commercial sectors.“Private-sector security experts have identified limited ongoing cyber activity from China but have not verified state sponsorship or the use of exfiltrated data for commercial gain,” he added. Clapper remains skeptical however: “Russia and China continue to have the most sophisticated cyber programs. China continues cyber espionage against the United States. Whether China’s commitment of last September moderates its economic espionage remains to be seen.” During a September 2015 testimony in front of the Senate Armed Services Committee, Clapper noted that the agreement was “good first step,” but unequivocally answered the question whether it would eliminate Chinese state-sponsored cyberattacks with a resounding “No.” “Such malicious cyber activity will continue and probably accelerate until we establish and demonstrate the capability to deter malicious state-sponsored cyber activity,” Clapper said back in September. During his February testimony, Clapper emphasized that Chinese cyber attacks are continuing: “It’s our responsibility to ensure that our policymakers and particularly the Department of Defense are aware of this hemorrhage, if you will, of technological information that the Chinese purloined.” According to Clapper, foreign actors in cyberspace “remain undeterred from conducting reconnaissance, espionage, and even attacks in cyberspace because of the relatively low costs of entry, the perceived payoff, and the lack of significant consequences.”

#### Chinese attacks prevalent — now is key because technologies are advancing

Gertz 16 — Bill Gertz, senior editor of the Washington Free Beacon. Prior to joining the Beacon he was a national security reporter, editor, and columnist for 27 years at the Washington Times. senior editor of the Washington Free Beacon. Prior to joining the Beacon he was a national security reporter, editor, and columnist for 27 years at the Washington Times, 2016 ("China Continuing Cyber Attackson U.S. Networks," *Washington Free Beacon*, March 18th, Available Online at http://freebeacon.com/national-security/china-continuing-cyber-attacks-on-u-s-networks/, Accessed 06-30-2016, MEW)

Six months after China pledged to halt cyber espionage against the United States, Beijing’s hackers continue to conduct cyber attacks on government and private networks, the commander of U.S. Cyber Command told Congress. Despite a formal pledge made by Chinese leader Xi Jinping in September, “cyber operations from China are still targeting and exploiting U.S. government, defense industry, academic, and private computer networks,” Adm. Mike Rogers, the Cybercom chief, said in prepared testimony to a House Armed Services subcommittee on Wednesday. Rogers echoed comments on continued Chinese cyber attacks made by Director of National Intelligence James Clapper in February. Clapper said in Senate testimony that “it remains to be seen” if China will abide by the informal pledge made during a summit meeting in Washington with President Obama. Rogers said he agreed with Clapper that China’s commitment to halt cyber espionage attacks remains an open question. China has been linked by U.S. intelligence agencies to wide-ranging cyber attacks aimed at stealing information and mapping critical computer networks for future attacks in a crisis or conflict. Despite the Chinese hacking activity, the Obama administration has taken no action against China for years of large-scale cyber attacks that officials say have cost the nation billions of dollars in stolen intellectual property and compromised networks. Rogers also warned that nation states with advanced cyber warfare capabilities are taking steps to mask their cyber attacks by cooperating with non-government hackers. Unspecified nation states are expanding cooperation “with a much broader range” of hackers in a bid to hide the source of sophisticated cyber attacks. “I think this is in no small part an attempt to obscure what the real originator of the activity is,” he said. The use of surrogate hackers makes it more difficult for the U.S. government to confront foreign states about cyber attacks. “And they say, ‘It’s not us. It’s some criminal group; we don’t control all that,’” Rogers said. Rogers also disclosed new details about cyber attacks against the email system used by the military’s Joint Chiefs of Staff, an attack that officials have blamed on Russia. The July attack shut down an unclassified email server for 10 days and disrupted an email system used by 4,000 users on the network. Pentagon officials believe the attack came from Russian government hackers. “Ultimately we were able to defeat the [intrusion] attempt in almost 60 other networks simultaneously except in this one particular network,” Rogers said, noting that the final defense against cyber attacks is the user of a computer. “In this case we had a user who clicked on a link that I said ‘What would lead you to do this? Read this. It doesn’t make any sense.’” Because computer users in the Joint Staff clicked on an email link that downloaded a virus, the Pentagon was forced to spend time and money and limit use of the system. “We can’t afford to have this sort of thing,” Rogers said. Under questioning from Rep. Elise Stefanik (R., N.Y.), Rogers said he is “comfortable” that Cyber Command has enough military capabilities to counter cyber threats from Russia, China, and other states and entities. “I’ve yet to run into a threat scenario that we couldn’t deal with,” he said. But Rogers voiced worries about his command having enough forces to deal with the threats. “What concerns me is capacity—how much of it do you have and as the threats proliferate, our ability to deal with high-end, simultaneous complicated threats, that’s probably the biggest limiting factor right now,” he said.

### They Say: “Cyberattacks Don’t Escalate”

#### Cyber conflicts go kinetic — loss of communications networks causes SCS conflict

Segal and Lan 16 — Adam Segal, Maurice R. Greenberg Senior Fellow for China Studies and Director of the Program on Digital and Cyberspace Policy at the Council on Foreign Relations, Tang Lan, Deputy Director at the Institute of Information and Social Development, China Institutes of Contemporary International Relations, 2016 (“Can the United States and China de-conflict in cyberspace,” *War on the Rocks*, April 27th, Available Online at <http://warontherocks.com/2016/04/can-the-united-states-and-china-de-conflict-in-cyberspace>, Accessed 06-27-2016, AW)

It is not hard to imagine cyber issues becoming intertwined with a crisis that spirals out of control. For example, U.S. and People’s Republic of China (PRC) forces are in close contact in the South China Sea, and cyberattacks could cause an incident to escalate rapidly. Hackers could target communication, computer, and transportation networks, degrading not only Beijing’s and Washington’s ability to control their forces in the field, but also their ability to signal to the other side their intentions to escalate or de-escalate the conflict. Non state actors, often known as patriotic hackers, could further confuse the situation as policy makers would have a difficult time differentiating between official and independent attacks. Additionally, a cyberattack that causes physical damage or widespread economic disruption could create domestic pressure for action that leaders in Washington and Beijing would have a hard time ignoring.

### They Say: “Cooperation Solves Cyber Norms”

#### U.S.-China cyber cooperation is key to international rules and oversight mechanism

Xinbo 14 — Wu Xinbo, Professor and Director of the Center for American Studies at Fudan University, Shanghai, China, an editorial board member of The Washington Quarterly, 2014 (“Agenda for a New Great Power Relationship,” *The Washington Quarterly*, Spring, Available Online at <https://www.ciaonet.org/attachments/24674/uploads>, Accessed 06-24-2016, AS)

The United States has long accused China of launching cyber attacks against its national security as well as commercial targets, while China has repeatedly denied such accusations and claims itself also a victim of cyber attacks from other countries, among which the United States ranks first. The Snowden revelation suggests that the U.S. National Security Agency (NSA) conducted many cyber attacks against Chinese targets,12 confirming Chinese complaints. While neither Beijing nor Washington would openly acknowledge their cyber espionage on each other, the Snowden episode could provide an opportunity to convert a cause for conflict into the basis for a dialogue that takes place on a more equal footing.

In July 2013, China and the United States held the first meeting of the bilateral Cyber Working Group. The two sides discussed issues of mutual concern and decided to take practical measures to enhance dialogue on international norms and principles in order to guide action in cyberspace, and to strengthen the Computer Emergency Response Team (CERT), a mechanism that deals with computer security incidents. With the first meeting of the Cyber [end page 75] Working Group described as “candid, in-depth, and constructive,” the two sides agreed to hold sustained dialogue on cyber issues.13

Given the fact that cyberspace is a new field in which international rules and an international oversight mechanism do not exist, many state and non-state actors have taken advantage of the situation to pursue their respective goals. This not only hurts the national interests of many countries, China and the United States alike, it also undermines the stability of cyberspace—a new but increasingly important global commons in the 21st century. It is therefore desirable that Beijing and Washington not only exercise self-restraint in their respective cyber activities, but also help promote the establishment of international rules and international oversight mechanisms, a vital public good that the great powers should provide in the era of information.

### They Say: “Cooperation Now/Cyber Agreement Solves”

#### No effective US-China cyber cooperation now

Lieberthal and Singer 14 — Kenneth Lieberthal, a senior fellow in Foreign Policy and Global Economy and Development at Brookings, former professor at the University of Michigan, has a bachelor’s from Dartmouth College, and a master’s and doctorate in political science from Columbia University, and Peter W. Singer, Senior Fellow at the Brookings Institution, Director of the Center for 21st Century Security and Intelligence at the Brookings Institution, received his Ph.D. in Government from Harvard University and an A.B. from Princeton's Woodrow Wilson School of Public and International Affairs, 2014 (“Cybersecurity and U.S.-China Relations,” *John L. Thornton China Center* and *21st Century Defense Initiative* at *Brookings*, February, 06-24-2016, p. 13-14, AS)

In short, U.S. concern about cybersecurity has reached a fever pitch— to the extent that the U.S. government’s 2011 Office of the National Counterintelligence Executive report specifically names China as the “most active and persistent” perpetrator of cyber intrusions into the United States.8 In the press, the mood is best captured by the depiction of a cyberattack as a massive pixilated mushroom cloud looming over every American city (as the cover of the July 2010 Economist magazine had it). Similarly, in senior policy circles, malware has been described as “like a WMD [weapon of mass destruction]” (Sen. Carl Levin, chair of Senate Armed Services Committee), able to “destroy our society” [end page 4] (former national security advisor Brent Scowcroft), meaning it should be looked at as “an existential threat” (Adm. Mike Mullen, former chairman of the Joint Chiefs of Staff).9 Indeed, many are now framing the U.S.-China relationship in this space as a digital echo of the Cold War between the U.S. and USSR of a past generation.10

While the Cold War metaphor is certainly a flawed parallel, as scholars at Brookings have recently argued,11 concern has grown to view the cyber threat on that scale. President Barack Obama’s 2011 Cyberspace Policy Review declared that “cybersecurity risks pose some of the most serious economic and national security challenges of the 21st century.”12 And, in turn, there have been a host of new U.S. legislative initiatives and the launch of a new cyber deterrence strategy by the U.S. military to accompany the creation of its U.S. Cyber Command. While it did not specify any individual nation, the Pentagon Strategy for Operating in Cyberspace was clearly keyed to China as among the many threats it foresaw in this realm.13 It sought to lay out a cyber deterrence doctrine clearly targeting state actors, including leaving open the option for escalation to traditional military means in the physical realm if the U.S. ever felt it suffered too dearly in the cyber realm.

### They Say: “Norms Don’t Stop Attacks”

#### US-China cooperation on international cybersecurity norms is essential to global cybersecurity

Jong-Chen 16 — Jing de Jong-Chen, a Senior Director for Global Security Strategy and Diplomacy in the Cloud and Enterprise Division at Microsoft, Board Advisor at Executive Women Forum, has a Bachelor of Science (B.S.), Computer Science and Engineeing from Beijing University of Aeronautics and Astronautics, 2016 (“US-China Cybersecurity Cooperation Needs to Move More Rapidly,” *Digital Futures Project* at *The Wilson Center*, April, Available Online at <https://www.scribd.com/doc/310936704/U-S-China-Cybersecurity-Cooperation-Needs-to-Move-More-Rapidly>, Accessed 06-22-2016, AS)

When U.S. President Barack Obama and Chinese President Xi Jinping joined other world leaders at the 2016 Nuclear Security Summit, controlling proliferation wasn’t the only global issue on their minds. During the summit, Presidents Xi and Obama also held side meetings to discuss cybersecurity, identifying ways that China and the United States can continue working together to address the threat of cyberattacks and cybercrime—both within their own borders and across the entire global community.

The meeting was no outlier; the two countries consider cybersecurity a top priority for bilateral relations. In recent years, state-sponsored cyberattacks, along with those carried out by terrorists and increasingly sophisticated criminal groups, have escalated to such a degree that they now pose a serious global threat to national security, public safety, and economic stability. As societies adopt even more technology-based services to help manage interpersonal and business communications, industrial control systems, the Internet of Things, and critical infrastructure, the risk posed by targeted and persistent cyber threats will continue to grow. No wonder so many informed observers, including world leaders from China, Russia, the European Union and the United States, have compared the challenge of managing cybersecurity to that of negotiating nuclear arms-control treaties. [end page 1]

Of course, despite a few key similarities between the threats of nuclear and cyber warfare, there are distinct differences that make achieving consensus on cybersecurity uniquely complex:

* While nuclear weapons remain state-owned and state-controlled, anyone with sufﬁcient knowledge and the right technology, which is relatively inexpensive and easy to obtain, can launch a cyberattack.
* Nuclear attacks are devastating but never secret; cyberattacks can be both. And because they can take many different forms, they are sometimes hard to identify and may do serious damage before they are discovered.
* The idea of an anonymous nuclear attack is unthinkable, but it is often impossible to tell where cyberattacks are coming from, especially if the aggressors use proxies to hide their identities.

On top of those issues, cybersecurity is so challenging because of the diverse perspectives from which nations view underlying questions of Internet governance and sovereignty. China, for example, believes that governments should have absolute control over the Internet and its use within their borders. Conversely, the United States sees the Internet as a global network without borders, which enables the free ﬂow of information and provides for unrestricted cross-border commerce and communication.

Yet there are two unassailable facts that transcend these political and philosophical differences, offering a foundation for shared progress: 1) the Internet is an economic engine that is now an integral component of the global economy, and 2) it is in every nation’s best interest to keep the Internet working efﬁciently, without unnecessary restrictions that would hamper global economic growth.

What’s needed is a set of cybersecurity policies and international norms that enable all countries to protect their citizens and critical infrastructure from cyberattacks, defend against economic and military espionage, and safeguard their national security. That said, we should be wary of laws that grant government powers that could isolate users, violate privacy, increase the cost of delivering information and services, restrict innovation, disrupt global trade, or prevent sustained economic growth. [end page 2]

As two of the world’s most inﬂuential nations, China and the United States share responsibility for leading the effort to establish such policies and norms—work that began in earnest when the two countries agreed in 2015 to neither conduct nor condone the cyber theft of intellectual property or business secrets, and to abide by what President Xi called “norms of behavior” in cyberspace. President Obama, who called the agreement a “work in progress,” said that China and the United States can now work with other world powers to develop a clear and enforceable “architecture to govern behavior.”

As the nations of the world work to strengthen cybersecurity, both nationally and internationally, ﬁve key considerations can guide policy makers:

* Collaboration: As governments develop policies to address cybersecurity concerns, they would beneﬁt from consulting and collaborating with the private sector and academia. Private-sector companies produce many of the innovations that make the cyber world possible; they want to protect their intellectual property and keep their customers’ information private and secure. Nations may always take the lead on establishing a global cybersecurity framework, but the private sector has a real stake in the outcome and can contribute to strategies and solutions.
* Harmonization: The Internet is global in scope and must remain ubiquitous to realize its full potential. Jurisdictions and national sovereignty are important considerations in protecting cyberspace, but borders can neither contain nor control cyberattacks. That’s why the global community needs a common set of rules under which cyber incidents and cybercrimes can be swiftly addressed. Technology companies that operate globally must obey the laws—and respect the rights of consumers and companies—in the countries where they do business. Yet such companies often ﬁnd themselves dealing with laws that conﬂict with each other, and so in seeking to comply with one law they may violate another. Harmonized standards will promote understanding, enhance predictability, and enable better public/private collaboration.
* Best practices: In developing effective cybersecurity policies, governments don’t have to start from scratch. By partnering with the private sector, they can build on existing best practices for mitigating cyber threats and take advantage of tested frameworks, advanced security strategies, and innovative technology solutions.
* Risk reduction: Reducing geopolitical risk is an essential aspect of diplomacy. Because risks are not usually managed on a global scale, however, it is a concept rarely addressed by public policy or international law. Yet because of the widespread availability of the Internet, geopolitical risk reduction must become a core component of nations’ cybersecurity work.
* Trust and transparency: Governments can build trust, among their own citizens and throughout the global community, by demonstrating greater transparency in their cybersecurity practices.

As nations work to make cyberspace more secure without restricting economic growth, it is vital that the public and private sectors work together to ﬁnd solutions, and that technology companies continue to play a central role in safeguarding the cyber [end page 3] environment they are helping to create. When the citizens of all nations feared nuclear annihilation during the Cold War, the global community came together to make the world more secure. The threats from cyberattacks that we face today may be less apocalyptic, but making the world safer from those threats is no less challenging. Once again, it will take common action to ﬁnd the answer.

### They Say: “Treaties Solve”

#### Norms provide the best mechanism for cyber cooperation – treaties fail

Eichensehr 15 - Visiting Assistant Professor, UCLA School of Law. (c) 2015, Kristen E. Eichensehr. The author thanks Raechel Anglin, Jack Balkin, Sarah Cleveland, Ashley Deeks, Oona Hathaway, Harold Hongju Koh, David Koplow, Richard M. Re, W. Michael Reisman, Michael N. Schmitt, Phil Spector, Peter Trooboff, Stephen Zamora, and participants in the American Society of International Law Southeast Interest Group Junior-Senior Workshop for helpful conversations and comments. The author is grateful for the assistance of Clay Greenberg, Sean Quinn, Justin Simeone, and the editors and staff of The Georgetown Law Journal for their suggestions and assistance. This Article reflects developments through November 2014 when it was finalized for publication, and any errors are the author's alone. January, 2015 The Cyber-Law of Nations Copyright (c) 2015 Georgetown Law Journal 103 Geo. L.J. 317 Available Online on Lexis Nexis

If the absence of a governance regime is unacceptable, but a broad multilateral treaty is impossible, development of norms to govern behavior in the cyber domain may be the best--or only--option. Unlike a meticulously negotiated treaty text, norms are general principles, not precise rules. n245

However, norm development is attractive for several reasons.

First, norms are easier to develop than a treaty and therefore may provide a faster route to establishing at least a partial governance system. Unlike a treaty, which requires broad agreement and may take years to negotiate, norms can arise through states acting individually, bilaterally, regionally, or multilaterally and without agreement of all states. n246 Norms may develop through unilateral policy declarations, such as states' issuance of cyberspace policies or speeches by government officials. n247 Norms may also arise through actions and statements of groups of states or simply between two states. Bilateral declarations might include joint communique's n248 or, for example, the addition of cyber attacks as triggers for the provisions of the U.S.-Australia mutual defense treaty. n249 On a regional level, NATO in 2011 issued a "Policy on Cyber Defence," which makes clear that "NATO will defend its territory and populations against all threats, including emerging security challenges such as cyber defence" and that NATO will provide assistance if its members suffer a cyber attack. n250 In a declaration accompanying a meeting of heads of state in September 2014, NATO further clarified its position that "international law, including international humanitarian law and the UN Charter, applies in cyberspace." n251

Such declarations have the potential to emerge from groups that are not [\*362] simply composed of like-minded allies. For example, in June 2013, the U.N. Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security achieved consensus on the very general principle that "[i]nternational law, and in particular the Charter of the United Nations," applies in cyberspace. n252 Although the generality of the agreed statement leaves much unclear about the application of international law in practice, the declaration is significant because it represents agreement by all fifteen of the GGE member states, n253 including Russia and China, which had not previously conceded that international law applies to cyberspace at all. n254

The informality and multistage process of norm emergence also has the potential to provide a greater voice to developing countries and to non-governmental actors. In bilateral interactions with, for example, the United States, United Kingdom, or China, developing countries may be able to exert a stronger influence on norm development than they would at a single conference to develop a broad cyber treaty. n255 Enfranchisement of developing countries in norm creation may promote buy-in to the resulting norms and avoid later problems, like those surrounding the Budapest Convention, n256 whereby developing countries are pressed to accept a fait accompli. Of course, efforts to recruit developing and other as yet undecided countries to one set of norms or another may provide an additional arena of competition for the United States and its allies, and China, Russia, and their allies. n257

Second, norms can develop through and evolve with state practice. Much remains unknown about states' capabilities, which change with technological advances. A treaty aimed at current capabilities risks becoming out-of-date, but [\*363] norms provide a more nimble mechanism to account for changes in technology and improved knowledge about states' capacities in cyberspace. For example, state practice in responding to cyber events will help to develop customary international law regarding what constitutes a use of force or an armed attack. n258 Such state practice will help to establish how states will treat similar future incidents.

Also, states acting rationally in their own self-interest over time may come to the same conclusion about acceptable behavior. n259 For example, the United States currently advocates rule-of-law norms prohibiting intellectual property theft and other criminal actions in the cyber domain, including by supporting broad adherence to the Budapest Convention. n260 As China, Russia, and other countries become increasingly dependent on cyber infrastructure and innovation, harms to their own citizens and businesses from cyber intrusions and cybercrime may cause them to shift toward the U.S. position of rule of law in cyber. n261 Independent discovery or "independent learning" of norms by individual states may pave the way for future formal agreement. n262

Finally, norms can fulfill some of the same purposes as a treaty, including coordinating state behavior, promoting stability and order in the international system, and decreasing the risk of unintended conflict. n263 The potentially decentralized nature of norm formation, described above, raises the possibility that [\*364] conflicting norms may emerge. But even in that circumstance, norms have the potential to serve a coordinating function and foster valuable clarity about states' actions. The U.S. International Strategy for Cyberspace advocates norm development for this reason. The Strategy notes that the world's growing dependence on cyberspace has "not been matched by clearly agreed-upon norms for acceptable state behavior in cyberspace." n264 It explains that "[i]n other spheres of international relations, shared understandings about acceptable behavior have enhanced stability" and brought "predictability to state conduct, helping prevent the misunderstandings that could lead to conflict." n265 The Strategy further asserts that norms "will diminish misperceptions about military activities and the potential for escalatory behavior." n266

The United States has recently taken bilateral steps with China and Russia that explicitly focus on decreasing misperceptions. In June 2013, the United States and Russia announced an agreement "to reduce the risk of conflict in cyberspace through real-time communications about incidents of national security concern." n267 The agreement provides for communications and information sharing between U.S. and Russian computer emergency-response teams, a direct channel for urgent communications about cyber exercises and incidents, a direct communications link between the U.S. cyber coordinator and his Russian counterpart (a repurposing of the Cold War nuclear "hotline"), and a working group "on issues of threats to or in the use of" information and communications technologies (ICTs) that will discuss emerging threats and coordinate joint exercises in order to "strengthen confidence." n268 The United States and China also established a working group to discuss cybersecurity issues, though China suspended its participation in the wake of the May 2014 U.S. indictments of Chinese military officials for hacking U.S. companies. n269

## Relations Advantage

### 1AC — Relations

#### Contention \_: US-China Relations

#### First, a framework for CERT cooperation would prevent hiccups in relations and bolster cyberdefense.

Mussington 15 — David Mussington, Adjunct Professor in Political Science at Georgetown University, Fellow at the RAND Corporation, Ph.D. in Political Science from Carleton University, M.A. in Economics and Political Science from the University of Toronto, 2015 (“The Missing Compliance Framework in the 2015 U.S.-China Cybersecurity Agreement,” *Institute for Defense Analysis,* November 18th, Accessible Online at <https://www.ida.org/~/media/Corporate/Files/Publications/IDA_Documents/ITSD/2015/D-5648.ashx>, Accessed On 06-22-2016, MA)

A concrete compliance framework would be a significant diplomatic and political breakthrough – indicating that both sides had considered the costs of continuing the status quo – selecting instead an alternate course with agreed facts, definitions, and dispute discussion (if not resolution) procedures. Further, such a bilateral framework might partially insulate the relationship from temporary hiccups – caused by the discovery of ongoing activities (legacy) that had yet to be reined in consistent with the new rules of the game. CERT-to-CERT-type contacts would further deepen the linkage between bilateral agreements to refrain from proscribed actions in cyber and operational exchanges on data that support non-controversial investigations of cyber-crime. Lastly, such a framework could provide a mechanism for discussion of IP rights holder injury and remediation options. In this way the compliance framework would provide added support to law enforcement cooperation on cyber-crime already established, as well as aligning well with norms emerging from the United Nations Group of Governmental Experts (GGE) process.

#### Second, cybersecurity is the most important issue for relations and effects the entire relationship.

Lieberthal and Singer 14 — Kenneth Lieberthal, a senior fellow in Foreign Policy and Global Economy and Development at Brookings, former professor at the University of Michigan, has a bachelor’s from Dartmouth College, and a master’s and doctorate in political science from Columbia University, and Peter W. Singer, Senior Fellow at the Brookings Institution, Director of the Center for 21st Century Security and Intelligence at the Brookings Institution, received his Ph.D. in Government from Harvard University and an A.B. from Princeton's Woodrow Wilson School of Public and International Affairs, 2014 (“Cybersecurity and U.S.-China Relations,” *John L. Thornton China Center* and *21st Century Defense Initiative* at *Brookings*, February, 06-29-2016, MA)

But the United States and China are the two most significant national players in this sphere. Moreover, these two leading states represent very different views on the proper use and future of the Internet. We therefore feel that thinking through these issues in a U.S.-China context can provide a useful way to develop approaches that should then be discussed more broadly, with the goal of ultimately establishing global norms and implementing mechanisms to bring greater order and security to those parts of the cyber realm where this is feasible.

More importantly, the spillover effect of cybersecurity on the broader U.S.-China relationship is also perhaps more critical than for any other bilateral relationship. This is both because of the enormous importance of U.S.-China relations in the emerging world order and, in turn, the growing role of cyber issues in eroding strategic trust and poisoning public and elite attitudes. If this trend can be reversed through improved engagement by the U.S. and China on cybersecurity, the outcome would be a “triple win.” It would bolster U.S.-China bilateral relations, serve as a crucial building block for multilateral efforts in the cyber arena, and also aid in broader US-Chinese engagement on other issues of importance, like global finance and the environment, where the two nations must learn to work better together.

#### [Insert China Relations impact]

### They Say: “Doesn’t Solve Relations”

#### Cooperation on cybersecurity makes or break long-term Chinese relations

Lieberthal and Singer 14 — Kenneth Lieberthal, a senior fellow in Foreign Policy and Global Economy and Development at Brookings, former professor at the University of Michigan, has a bachelor’s from Dartmouth College, and a master’s and doctorate in political science from Columbia University, and Peter W. Singer, Senior Fellow at the Brookings Institution, Director of the Center for 21st Century Security and Intelligence at the Brookings Institution, received his Ph.D. in Government from Harvard University and an A.B. from Princeton's Woodrow Wilson School of Public and International Affairs, 2014 (“Cybersecurity and U.S.-China Relations,” *John L. Thornton China Center* and *21st Century Defense Initiative* at *Brookings*, February, 06-24-2016, p. 16, AS)

In sum, distrust of each other’s actions in the cyber realm is growing between the U.S. and China, and such distrust easily spills over into broader assessments of the other country’s long term intentions. It is heightened by the link between the cyber domain and key values like individual privacy on the U.S. side and concerns with internal stability on the Chinese side. Even more, the potentially poisoning effect of cybersecurity on the relationship is occurring at a time when there is genuine uncertainty about the degree and speed of changes in the global balance of power. The disagreements feed into the anxieties on all sides as to whether America and China will have a basically cooperative or antagonistic relationship over the coming several decades.25

In traditional relations between two powers, the intersection of capability, vulnerability, and intention directs whether the states look at each other as partners or threats. Thus, the stakes in this fundamental issue could hardly be higher. Policymakers and publics on both sides must face the fact that, at this point, developments in the cyber realm are contributing to tensions rather than enhancing confidence in each side’s ability to find ways to cooperate with the other to handle the major issues we collectively face in a changing world.

### They Say: “Cyber Not Key”

#### Cooperation on cybersecurity key to US-Sino relations — spills over

Jong-Chen 14 — Jong-Chen, Jing De, senior director and domain expert on global cybersecurity policy and strategy at Microsoft Corporation, 2014 ("U.S.-China Cybersecurity Relations: Understanding China’s Current Environment," *Georgetown Journal of International Affairs*, September 15th, Available Online at http://journal.georgetown.edu/u-s-china-cybersecurity-relations-understanding-chinas-current-environment/, Accessed 6-29-2016, MW)

Recommendations U.S.-China relations are facing a challenging period. How do the United States and China move away from the mistrust that currently governs the relationship? How could the U.S. and China find common ground when there are clearly disagreements over cyber sovereignty and Internet use? With fundamentally different political and social systems, how would the U.S. and China align their national security interests with global benefits to protect cyber infrastructure and trade? What security policies and legal frameworks are needed to promote global collaboration and supply chain trust? The following recommendations are provided from an industry perspective as potential common areas for both sides to consider, while recognizing the different political and economic structures and cybersecurity goals of each country. Establish a leadership and relationship model. A cybersecurity leadership and relationship model is needed to normalize the communication and conflict resolution between both countries. It should involve U.S. and Chinese stakeholders from both the public and private sectors, including policy makers, senior domain experts from technical, legal, trade and diplomatic fields with security expertise. The goal is to identify activities that are considered threatening for both countries and keep government-to-government and government-to-industry communication channels open. There are many existing international models for such working partnerships that could be used to create a structure for dialogue and to work through the complex challenges of cybersecurity. Develop and adopt globally recognized best practices to address supply chain trust. These would help both Chinese and U.S. industries participate and innovate in the broader global ICT economy. Governments and industry could better secure their networks by establishing a proper security assurance model, operational procedures and protections. Further, the use of widely available security technologies such as public and well vetted commercial encryption and authentication management would make it harder for hackers to compromise confidential data, providing a higher level of security for governments, businesses and individuals alike. Expand the role of industry in cyber norms and cybersecurity solutions. Expanding public-private partnerships and leveraging private sector expertise is critical to improve global cybersecurity. For the past decades, the global technology industry has been a major driving force and contributor to the Internet economy and the development of security standards and best practices, regardless country of origin. The technology industry should be trusted to carry out the future innovations to boost productivity, connect people and improve quality of life worldwide. Most of all, the industry should become partner to protect global critical infrastructures. Build international partnerships to combat cybercrime. Law enforcement collaboration across international borders is critical for addressing global cybercrime. Judicial exchanges and specialized legal training and partnerships with law enforcement would increase the effectiveness of prosecuting cybercrime based on national and international laws, and would identify gaps in the legal process of both countries that may hinder prosecution. Industry should also be encouraged to deliver services and innovation to reduce user risks and minimize the damages of cybercrime.

#### Cybersecurity intersects with all other issues — economics and intellectual property

Robledo 16 — Christian Robledo, International studies scholar, under the guidance of David Bachman, professor of International Studies at Washington University, 2016 (“Balancing Cooperation and Competition: A New Era In U.S.-China Relations,” *The Henry M. Jackson School of International Studies at University of Washington*, March, Available Online at <https://digital.lib.washington.edu/researchworks/bitstream/handle/1773/36217/TaskForceAReport-2016-Bachman.pdf?sequence=1>, Accessed on 6/29/16, MEW)

Cybersecurity has been and continues to be among the most pivotal issues that influence United States relations with China. Over the past few years, numerous private and public sector networks have been the target of Chinese hacking which has resulted in the theft of intellectual property, personal data, military information and other invaluable assets, costing billions of dollars in damage. A recent report, sponsored by Hewlett Packard Enterprise, estimated that the annual average cost of cyber crimes to 58 benchmark U.S. public and private organizations was $15.4 million per company.1 The study analyzed a diverse group of industries that ranged from those in the financial services, to those in hospitality. The report also concluded that the U.S., compared to other countries, continues to rank highest in costs associated with cyber crime. Reports such as the one mentioned above highlight the vulnerability of private and public networks and illustrate the need to fortify cyber defenses. The nature of cyberspace, specifically cyber attacks, however, pose a variety of challenges that makes them extremely difficult to deal with. Those challenges include, but are not limited to: lack of agreement over critical terminology (e.g. what constitutes a “cyber crime,” “cyber attack,” “cyber threat,” etc.), matters of attribution (i.e. where a threat or attack emanates from and whether it involves state or nonstate actors), and challenges associated with time, i.e. the ability of policymakers to develop and pass cyber defense legislation or budgets lag far behind the rapid rate at which cyber attack capabilities evolve.

### They Say: “Economics K2 Relations”

#### Cybersecurity accesses trade in the U.S.-Relationship

Segal 15 — Adam Segal, Maurice R. Greenberg Senior Fellow for China Studies and Director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations, 2015 ("Stabilizing Cybersecurity in the U.S.-China Relationship," *The National Bureau of Asian Research*, September 14th, Available Online at http://nbr.org/research/activity.aspx?id=605, Accessed 06-27-2016, AW)

These attacks fall into three categories. The majority are the cyber-enabled theft of intellectual property, business strategies, and trade secrets. There is also a widespread campaign of political and military espionage such as the hack of the U.S. Office of Personnel Management, which may have exposed the records of over twenty million current and former federal employees. In addition, the members of the People’s Liberation Army Unit 61398 have reportedly penetrated the networks of natural gas pipelines and electric utilities, possibly to map the potential future battlefield or prepare for a destructive attack. The cybersecurity issue has also spilled over into trade relations. In part motivated by disclosures of U.S. cyberespionage against Chinese targets made by the former National Security Agency contractor Edward Snowden and in part a reflection of a long-held techno-nationalism, Chinese policymakers have introduced a number of regulations designed to reduce dependence on foreign suppliers for critical technologies. New banking regulations, for example, and the draft antiterrorism and national security regulations in China require companies to share source code and build backdoors into encrypted products in an effort to make technology “secure and controllable.” Although the bank regulations were suspended in April, protectionism remains tightly linked to cybersecurity concerns.

# Answers to Off-Case Positions

## Elections DA

### 2AC — Link Non-Unique

#### Hillary is already hard on Chinese cybersecurity

Ekberg 15 ― Brett Ekberg, research associate in the Digital and Cyberspace Policy Program at the Council on Foreign Relations, 2015. (“Five predictions for cybersecurity's role in the 2016 presidential race”, CFR, August 31st, 2015, Available Online at: <http://blogs.cfr.org/cyber/2015/08/31/cybersecurity-on-the-campaign-trail-five-predictions-for-2016/> Accessed 6-30-16)

The rhetoric against China will continue and escalate

While we likely won’t see Lincoln Chafee demand that Xi Jinping tear down the Great Firewall, we should expect to see many of the candidates continue their anti-China rhetoric, particularly if future data breaches are linked to the country, confirmed or otherwise. Republicans blamed the president’s “weak” China policy for the recent OPM hack and were quick to demand that the administration respond. Among democratic candidates, Hillary Clinton has taken the toughest stance on China’s actions in cyberspace, accusing the Chinese of “trying to hack everything that doesn’t move in America.”

In a presidential election where republican voters have named national security their top concern, and where democrats may see speaking out against China as a way to counter GOP rhetoric that their party is weak on that issue, it would be a surprise to see a candidate soften his or her language prior to November 2016.

## Cyber Sanctions CP

### 2AC — Cyber Sanctions CP

#### Perm — do both. Sanctions in some areas and cooperation in others aren’t mutually exclusive.

#### The counterplan doesn’t solve cybersecurity or relations.

Yi 15 — Shen Yi, Associate Professor and Deputy Director of the Center for Cyber Governance at Fudan University, 2015 (“For China and the U.S., Cyber Governance Is Better Than Cyberwar,” *The World Post,* September 22nd, Accessible Online at <http://www.huffingtonpost.com/shen-yi/cyber-governance-cyber-war-china_b_8177732.html>, Accessed On 06-29-2016)

A more responsible way of looking at U.S.-China cyber relations would be to recognize that cyber conflicts and cooperation between the two countries as the “new normal.” Naturally the best way to manage the relationship should be to listen to each other and treat each other as equal partners. Only on that basis, can we begin to construct the much needed rules to govern the global cyber commons.

The strategy of pressuring China, forcing it to make concessions, will not become a lasting model of U.S.-China interaction in the cyberspace, even though the U.S. still enjoys significant strategic advantage in global affairs.

The essential spirit of the USCIIF is cooperation. Only by exploring new dimensions of cooperation in the digital economy, could the U.S. and China respond to new threats to cybersecurity, and promote mutual development and prosperity. It is unwise to call China’s overture a “conspiracy” and dismiss it as “flexing tech muscles.”

As a Chinese saying goes, “the world is more beautiful when one adopts a long-term view and keeps an open mind.” Now, Silicon Valley is leading. Will Washington follow?

#### Sanctions Fail — they empirically haven’t had an effect on other countries like North Korea or Iran.

#### US pressure fails — concessionary engagement is the better option.

Austin 15 — Greg Austin, Professorial Fellow at the East-West Institute, Professor at the Australian Center for Cybersecurity, 2015 (“The US-China cyberwar needs détente,” *Boston* Globe, August 30th, Accessible Online at <https://www.bostonglobe.com/ideas/2015/08/29/the-china-cyberwar-needs-detente/p8T9GFDjbW2GuJwlGjpIZP/story.html>, Accessed On 06-28-2016)

If China has been able to keep business-like relations with all other partners on cyber issues, in spite of its rampant cyberespionage against them, then why is its cyber relationship with the United States so much worse than with other major powers?

At one level, the answer is obvious: The United States can afford to be more strident in its diplomacy than any other Western country because it is more powerful. In addition, relative to most countries that are getting along better with China in cyber affairs, the United States also puts more stock in certain issues of principle, such as human rights protections in cyberspace or theft of intellectual property.

Washington also believes that it needs to stand up to China on such issues, not least because of the way in which China’s power is disturbing American allies in the Pacific. This is, after all, one motivation of the rebalance in US strategic policy.

Even so, the style and tone of current American cyber diplomacy toward China looks surprisingly messy. This is unexpected: US diplomacy toward China under Obama has generally been very impressively organized and thought through.

US perceptions about China in cyberspace hinge on a few mistaken beliefs. They include the notion that there are unambiguous norms in cyberspace that China is flagrantly violating; a failure to appreciate China’s deep insecurity in cyberspace; a lack of knowledge of America’s extensive cyberespionage and cyber military operations against China; and an inflation of the threat from China’s theft of intellectual property.

Of course, the US cybersecurity industry as a lobby group is very alert to all of the above and plays it for commercial gain. Yet officials rarely note that most cybersystems are inherently vulnerable and cannot be secured against a determined cyber adversary.

This is not to say by any means that China is without fault. Far from it. But what is equally undeniable is that the impact of the China cyberthreat relative to other threats is exaggerated by the US cybersecurity community.

All of this is particularly ironic, given the deep integration of the cyberindustry sectors of the two countries. China depends on the United States for its own cyber power. Meanwhile, leading American suppliers of communications and information technology are heavily dependent on China in their supply chain or even as a source of final manufacturing. Their level of involvement in China is so deep that they have even lobbied against US sanctions on China for cyber espionage.

The challenge from here? To unravel this entanglement of influences and to base future cyber diplomacy on a more sophisticated notion of the world as it is.

The Soviet-US detente in the Cold War era suggests that less outrage about mutual espionage, and cultivating a more nuanced appreciation of its limited impacts relative to the larger military threats, could lead to better — more realistic — relations.

#### Cyber sanctions against China fail and don’t influence behavior.

CNBC 15 — CNBC, major broadcasting network, citing Tristan Reed, East Asian Security Analyst with Stratfor, Byline: Everett Rosenfeld, 2015 (“Would cybertheft sanctions on China be effective?,” *CNBC,* September 14th, Accessible Online at <http://www.cnbc.com/2015/09/14/would-cybertheft-sanctions-on-china-be-effective.html>, Accessed On 06-29-2016)

But experts say that cyber incursions are often difficult to attribute to any region, let alone specific state- or company-sponsored actors.

While Stockton said he was hopeful that sanctions could begin to shift behavior from China and its corporate sector, others have expressed some doubt, especially in light of Chinese President Xi Jinping's apparent disregard of messaging—like the April executive order—from the White House.

"[Sanctions] are not likely to carry any effect outside of angering President Xi's constituents in China," said Tristan Reed, a security analyst with geopolitical intelligence and advisory firm Stratfor.

In fact, he added, any sanctions are unlikely to be particularly onerous for Beijing.

"The U.S. isn't going to impose wide sanctions on China, particularly with wider economic concerns now," Reed said, referring to worries that China may be losing its grip on an ongoing growth deceleration. "It's going to be difficult to find meaningful sanctions to impose."

#### Turn — sanctions for cybersecurity spark global protectionism.

Scissors 11 — Derek Scissors, Research Fellow for Asia Economic Policy at the Heritage Foundation, Resident Scholar at the American Enterprise Institute, Ph.D. in Political Science from Stanford University, 2011 (“China and Cybersecurity: Trojan Chips and U.S.–Chinese Relations,” *Heritage Foundation,* May 5th, Accessible Online at <http://www.heritage.org/research/reports/2011/05/china-and-cyber-security-trojan-chips-and-us-chinese-relations>, Accessed On 06-29-2016)

One drawback of restricting trade would be the costs incurred by the U.S. in terms of spending on import inspections and the loss of availability of certain goods. The defense community is often not well-positioned to anticipate the extent of these economic costs. People will not relinquish scarce resources voluntarily when the gains from doing so are not spelled out.

The second drawback is the reaction of American trade partners. American exports already suffer from undocumented national security justifications for protectionism. Were the U.S. to introduce a new set of potentially sweeping restrictions based on hidden national security requirements, the global trade environment would immediately and sharply deteriorate. Costs would be far higher than indicated by looking at American actions alone.

#### Global protectionism causes full-scale wars – escalates to WMD use.

Panzer ‘7 — Michael J. Panzer, a New York Institute of Finance faculty member and a graduate of Columbia University. Financial Armageddon: Protect Your Future from Economic Collapse, p. 137-138

The rise in isolationism and protectionism will bring about ever more heated arguments and dangerous confrontations over shared sources of oil, gas, and other key commodities as well as factors of production that must, out of necessity, be acquired from less-than-friendly nations. Whether involving raw materials used in strategic industries or basic necessities such as food, water, and energy, efforts to secure adequate supplies will take increasing precedence in a world where demand seems constantly out of kilter with supply. Disputes over the misuse, overuse, and pollution of the environment and natural resources will become more commonplace. Around the world, such tensions will give rise to full-scale military encounters, often with minimal provocation. In some instances, economic conditions will serve as a convenient pretext for conflicts that stem from cultural and religious differences. Alternatively, nations may look to divert attention away from domestic problems by channeling frustration and populist sentiment toward other countries and cultures. Enabled by cheap technology and the waning threat of American retribution, terrorist groups will likely boost the frequency and scale of their horrifying attacks, bringing the threat of random violence to a whole new level. Turbulent conditions will encourage aggressive saber rattling and interdictions by rogue nations running amok. Age-old clashes will also take on a new, more heated sense of urgency. China will likely assume an increasingly belligerent posture toward Taiwan, while Iran may embark on overt colonization of its neighbors in the Mideast. Israel, for its part, may look to draw a dwindling list of allies from around the world into a growing number of conflicts. Some observers, like John Mearsheimer, a political scientist at the University of Chicago, have even speculated that an “intense confrontation” between the United States and China is “inevitable” at some point. More than a few disputes will turn out to be almost wholly ideological. Growing cultural and religious differences will be transformed from wars of words to battles soaked in blood. Long-simmering resentments could also degenerate quickly, spurring the basest of human instincts and triggering genocidal acts. Terrorists employing biological or nuclear weapons will vie with conventional forces using jets, cruise missiles, and bunker-busting bombs to cause widespread destruction. Many will interpret stepped-up conflicts between Muslims and Western societies as the beginnings of a new world war.